EXHIBIT A

Defendants' Notice seeks to present three out-of-circuit cases in further support of their Motion to Dismiss: (i) *Zellmer v. Meta Platforms, Inc.*, 104 F.4th 1117 (9th Cir. June 17, 2024); (ii) *G.T. v. Samsung Electronics America Inc.*, No. 21 CV 4976, 2024 WL 3520026 (N.D. Ill. July 24, 2024); and (iii) *Martell v. X Corp.*, No.1:23-cv-05449, 2024 WL 3011353 (N.D. Ill. June 13, 2024). These out-of-circuit cases are factually distinguishable and—contrary to Defendants' assertions described further below—do nothing to "clarify"[1] their Motion to Dismiss arguments—which have already been fully briefed. For these reasons, and in light of the internal disagreement even within the Ninth Circuit on the legal issues for which Defendants present these three cases, these supplemental authorities should not be given any weight.

Defendants' Motion to Dismiss sets forth two arguments: (1) that Texas law (not Illinois law) applies here, and (2) that the Amended Class Action Complaint ("Complaint") fails to state a claim under the Illinois Biometric Information Privacy Act, 740 ILCS § 14/2 et. seq. ("BIPA"). *See* Motion to Dismiss Memorandum; *see also* "Plaintiffs' Opposition to the Motion to Dismiss," ECF No. 75 (setting forth reasons Defendants' arguments should be rejected). In their Notice, Defendants claim that these three cases advance their second argument, but they do not;

- ***Zellmer v. Meta Platforms, Inc.***: The Ninth Circuit found that the "face signatures [at issue] [we]re neither biometric identifiers nor information" based on (1) an unsettled interpretation of BIPA's definitions; and (2) the scant pleadings in the short operative complaint in that case. *Zellmer*, 104 F.4th at 1127.
- ***Martell v. X Corp.***: The Northern District of Illinois found that "[t]he fact that [the defendant's app] creates a unique hash for each photo does not necessarily imply

[1] *See* Defendants' Motion to File Supplemental Authority at 1 (arguing that the cases in their Notice "clarify critical disputed issues under the Illinois Biometric Information Privacy Act ('BIPA'), including the meaning of 'biometric identifier'").

that it is scanning for an individual's facial geometry when creating the hash" based on "[t]he absence of factual allegations to this point" in the relevant complaint. *Martell*, 2024 WL 3011353 at *2-3. Here, by contrast, the factual allegations are much more numerous and more thoroughly pleaded. *See* explanation *infra* at 3. But even so, the *Martell* court implicitly found that an "individual's facial geometry" *is* "biometric information" for the purposes of BIPA. *Martell*, 2024 WL 3011353 at *2.

- ***G.T. v. Samsung Electronics America Inc.***: While taking up the definition of "biometric identifier" for which Defendants advocate, the Northern District of Illinois acknowledged that the interpretation of BIPA definitions is not settled: "[c]ourts are divided on whether a plaintiff must allege [that] a biometric identifier can identify a particular individual, or if it is sufficient to allege the defendant merely scanned, for example, the plaintiff's face or retina." *Samsung*, 2024 WL 3520026, at *6 (collecting cases from the Northern District of Illinois, including cases that state that the supposed requirement that biometric identifiers must identify a unique person is not supported by BIPA's plain language).

These cases are so factually distinguishable from the instant case that they do not support Defendants' Motion to Dismiss arguments. *First*, Defendants allege that "*Zellmer* is [] applicable [because] Plaintiffs' allegations . . . fail to describe technology that can be used to specifically identify anyone."[2] *Zellmer*, with its short 15-page complaint and a plaintiff who never had a Facebook account (Zellmer's friends allegedly uploaded photographs of him), is factually distinguishable because Plaintiffs here, in a 116-page Complaint that thoroughly dives into the

[2] *See* Defendants' Notice at 3.

technology at issue, *do* allege that the biometric identifiers that Defendants collected from their accounts, including facial-geometry scans, identify them as individuals. *See* Plaintiffs' Amended Class Action Complaint and Request for Jury Trial ("Complaint"), ECF No. 60 ¶91 ("Facial recognition is a biometric technology that identifies facial vectors and features and matches them to an individual pre-enrolled in a database."); ¶94 ("A voiceprint is a digital model of the unique vocal characteristics of an individual."); ¶103 ("'Biometric information' consists of biometric identifiers used to identify an individual."); ¶138 ("Tinder marketed this [photo ID verification] feature to Tinder users as a 'vectorization' process that allowed users to verify their identity."). This level of specificity is not even required; any type of identifier enumerated in the BIPA statute should automatically qualify as a "biometric identifier" without further explication. *See* 740 ILCS 14/10 (stating explicitly, without qualification that, under BIPA, "biometric identifiers" include "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry"). As such, Plaintiffs' Complaint not only meets, but also surpasses, the BIPA standard, in a way that the *Zellmer*, *Martell*, and *Samsung* plaintiffs all failed to do.[3]

Second, Martell is distinguishable because the complaint in that case, also a scant 15 pages, failed to plausibly allege that defendant X Corp. (f/k/a Twitter) collected a "biometric identifier" as defined by the court's interpretation of BIPA. The *Martell* court distinguished the allegations before it from those in (i) *Carpenter v. McDonald's Corp,* explaining: "importantly, [in *Carpenter*] [p]laintiff alleges that McDonald's uses the AI and data to actually identify unique individuals.' [] The court found that these allegations were sufficient . . . [and (ii) s]imilarly, in *Rivera v. Google Inc.*, . . . [t]he court found that the allegation that Google created a biology-based face template of

[3] *See* Plaintiffs' Opposition to the Motion to Dismiss, §§II.A-B (explaining in detail how Plaintiffs have sufficiently pleaded their BIPA claims).

the individuals in the photos was sufficient to allege a scan of face geometry under BIPA."). *Martell*, 2024 WL 3011353 at *3. Defendants are thus wrong to assert that "*Martell* rejects *Carpenter v. McDonald's Corp.*"[4] On the contrary, *Martell* holds up *Carpenter* as an exemplar of a case in which plaintiffs' allegations were sufficient, just like those here.[5] Here, as emphasized *supra* (at 3) and *infra* (n.8), Plaintiffs do not merely allege that Defendants store face vectors (as alleged in *Martell*), but that Defendants *also* use them—in combination with other information in their databases—to verify users' identities (similar to the allegations in *Carpenter*).[6]

Finally, *Samsung* is factually distinguishable because plaintiffs there alleged that a Samsung photo app allowed its users to either upload template-less photos—which on their own are not biometric data or information—to the Samsung-controlled cloud, *or* keep them along with their derivative biometric data (face templates) "stored on the local Device (keeping open the possibility that Samsung received the [face template] Data elsewhere)." *Samsung*, 2024 WL 3520026, at *3 n.5. The *Samsung* court found that these allegations were "impermissibly speculative" as to whether Samsung actually received the alleged biometric data (face templates), and further noted that plaintiffs "do not argue that Samsung possesses the Data or took any active steps to collect it." *Id.* at *3 n.5, *6. Here, although discovery is needed to confirm the allegations,

---

[4] *See* Defendants' Notice at 3.

[5] *See* Complaint ¶188 n. 159 ("*Carpenter v. McDonald's Corporation*, No. 1:21-cv-02906, 2022 WL 897149, at *3 (N.D. Ill. Jan. 13, 2022) ('To the extent that defendants argue that it must have actually used Plaintiffs voiceprint and identified him as speaking to the voice assistant to implicate BIPA, the [c]ourt disagrees. In the [c]ourt's view, pursuant to the plain language of the statute, a defendant may violate BIPA by collecting a voiceprint that merely could be used to identify a plaintiff. The collection of a voiceprint-which is explicitly included in the definition of biometric identifier' without consent, even if not collected for the purpose of identifying that person, is a violation of the statute.'"); *accord* Plaintiffs' Opposition to the Motion to Dismiss at 21 (citing to *Carpenter* for the proposition that "[c]ourts routinely find allegations referring to defendants' patents that collect biometric information create a plausible inference that defendants did, in fact, collect biometric information.").

[6] *See* Complaint ¶¶92, 122, 138, 194.

Plaintiffs *do* plausibly allege that Defendants proactively collected app users' biometric data and then saved the data in their databases and servers, not just on users' devices, citing in various instances to publicly available patents that corroborate this allegation.[7] Moreover, while *Samsung* does adopt the *Zellmer* interpretation of "biometric identifier" under BIPA, it still readily acknowledges that this is a disputed issue among courts: "a 'biometric identifier' 'means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. "Courts are divided on whether a plaintiff must allege [that] a biometric identifier can identify a particular individual, or if it is sufficient to allege the defendant merely scanned, for example, the plaintiff's face or retina. . . . Unlike the definitions of 'biometric information' and 'confidential and sensitive information,' 740 ILCS 14/10, the term 'biometric identifier' does not include language stating it must be capable of 'identifying an individual.'" *Samsung*, 2024 WL 3520026, at *6-7. Thus, *Samsung* does nothing to clarify or confirm anything for this court other than to reaffirm that the appropriate touchpoint for this case is BIPA's plain statutory language. Moreover, while the *Samsung* opinion goes on to say that "the fact that the App performs face scans is not dispositive" regarding conformity with the "biometric identifier" definition, it *never* says that face scans *in combination* with other data would not be dispositive. *Id.* at *7. This is another way in which *Samsung* is distinguishable from the present case: here, Plaintiffs allege that Defendants store face prints (geometries, or vectors) *in combination with* other information in Defendants' databases in order to identify individual people, thus surpassing BIPA's requirements, as well as the pleadings of the *Zellmer, Martell,* and *Samsung* plaintiffs.[8]

---

[7] *See, e.g.,* Complaint ¶¶6, 75, 93, 95, 110, 144, 158, 187, 192 n. 166, 194, 205 n. 201-02, 240.
[8] *See, e.g.,* Complaint ¶6 ("The Dating Sites store user information and data on Match Group's shared servers."), ¶92 ("The face template that is extracted from the individual's face . . . is then matched to pre-existing templates in a database. . . to find the best match and confirm identity."), ¶110 ("All Dating Sites require users to create an account and 'personal profile' that must

For all these reasons, the cases cited in Defendants' Notice are inapposite, and the inferences drawn from them, as presented in the Notice, are misleading. This Court is respectfully urged to evaluate Defendants' Motion to Dismiss and Plaintiffs' corresponding opposition based on their respective briefs without further distraction.

include one or more photos of themselves . . . Defendants [] apply facial recognition technology to the user's photograph to extract, collect, store, and use the user's biometric information."), ¶122 (describing Defendants' "syncing [user] Facebook account[s] to the app" along with several data points from Facebook), ¶158 ("Defendants' patents also confirm that all Dating Site data, including but not limited to biometrics, is stored on the Defendants' databases"), ¶194 (describing how Amazon Rekognition's artificial intelligence tools power Defendants' ability to use dating app users' photo-derived face geometries and "feature vectors," saved in Defendants' databases, to identify individuals as a part of a "top picks" feature).